The ABC Conjecture

"I think I'm going to hurl."
- David Masser

Rough draft of an excerpt from the upcoming book
Trolling Euclid by Tom Wright

Chapter 1

ABC: What the Alphabet Looks Like When D Through Z are Eliminated[1],[2]

1.1 The Vomitous Beginning of a Beautiful Conjecture

Of all of the conjectures in this book, the ABC Conjecture is by far the least historic. Unlike 150-year old Riemann Hypothesis or the Twin Prime Conjecture whose age is measured in millennia, the ABC Conjecture was discovered in the rather recent and mundane year of 1985. Of course, an important open conjecture that was formed in 1985 is still a rather impressive proposition, as such a conjecture can then be said to have stumped mathematicians for almost 30 years. On the other hand, since the ABC is younger than I am, I can't really wax poetic about how the world was "a very different place when this conjecture was formed" unless I want to make myself feel really, really old. So that's kind of disappointing.

However, whatever gravitas the conjecture lacks because of its youthful age is no match for the amount of gravitas it lacks in how it was discovered.

[1]This is a variant of an old joke by former comedian Mitch Hedberg. RIP, Mitch

[2]Incidentally, every single exposition about the ABC Conjecture involves some variant of the joke "It's as easy as ABC!" I mean, *every single exposition* does this. Apparently, there are no other jokes that can possibly be made about the first three letters of the alphabet.

Yes, the ABC Conjecture is, to date, the only major math conjecture known to have been discovered at a cocktail party.

You see, mathematicians David Masser and Joseph Oesterle were at a cocktail party[3], drunk out of their minds[4], when they began to discuss a recent paper that had written the year prior about polynomials[5]. Masser and Oesterle started to think about what would happen if you took the paper and replaced every mention of "polynomial" with "integer". This took a while because Masser couldn't see straight and Oesterle was loudly singing Abba songs, but they felt that it was likely important, so they soldiered through it. Finally, after a bit of discussion and a lot of thought, it was Masser who, despite his inebriation, saw the light and realized what it was the duo could accomplish with this simple idea; in one of the memorable moments in math history, Masser then turned to his colleague said, "Hey Oesterle! BLAAGH!" and threw up all over Oesterle's shirt.

After cleaning up (and sobering up) a bit, Masser clarified that what he was going to say was, "Using the ideas from the paper, we should come up with a simple proposition about integers that would change the way we look at additive relations between integers and completely revolutionize the study of Diophantine equations. Also, BLAAGH!", and it was back to the mop and paper towels.

Once round two of cleanup had been done, Masser and Oesterle set to work. Realizing that Masser's idea was a good one, the pair sat down and hammered[6] out a stunning conjecture, outlining a fundamental relation between integers in some very straightforward equations that had somehow eluded mathematicians since the dawn of time. The equations they investigated were so simple that it was clear that there would be immediate applications throughout all of mathematics.

Then, for good measure, Masser threw up all over the page once more.

[3]This part is actually true

[4]This part might be slightly less true.

[5]Yeah, we mathematicians know how to party.

[6]Hammered, indeed.

1.2 Hold On - How Simple are We Talking Here?

The conjecture applies to nearly every equation of the form

$$a + b = c.$$

That's why it's called the ABC Conjecture.

1.3 Oh. Yeah, That's Pretty Simple.

See what I mean? That equation is bound to show up in quite a few places.

Chapter 2

Radical! Mason and Oesterle's Excellent Adventure Continues[1]

As you may have gathered from pretty much every word written in every chapter before this one, number theorists *love* primes. Like, really love primes, to the point where a restraining order might be required. That's just how we roll. So when we see an integer just sitting there like this:

$$600$$

our first instinct is to say , "Let's split the integer into prime factors!":

$$600 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5,$$

or, better yet,

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

You'd think that this would be enough prime-related carnage to satisfy our compulsion. Sometimes, it is. Other times, however, we might say, "No one cares about these exponents. All we want are primes! PRIMES!" In fact, we even have a function, called the radical (denoted $rad(x)$, so named because "Radical!" was considered a cool thing to say when the conjecture was made in 1985), where we take the prime factorization and strip the exponents:

[1] I think I may have left a few of my younger readers behind on the "Bill and Ted's Excellent Adventure" reference here. Well, too bad. The older readers are still scratching their heads at the Ke$ha reference from the Birch-Swinnnerton-Dyer section, so you can call it even.

$$rad(600) = 2^{\cancel{3}} \cdot 3 \cdot 5^{\cancel{2}} = 2 \cdot 3 \cdot 5.$$

Note that $2 \cdot 3 \cdot 5 = 30$, so we could write

$$rad(600) = 30$$

to get the same info across.

Want another example? Sure you do! Here's one:

$$112 = 2^4 \cdot 7,$$

so

$$rad(112) = 2^{\cancel{4}} \cdot 7 = 14.$$

That was awesome.

Note that the radical of a number is quite often much smaller than the original number. Of course, this isn't always the case:

$$rad(30) = 2 \cdot 3 \cdot 5 = 30,$$

$$rad(17) = 17,$$

but it's true often enough to be a useful tool in simplifying things considerably. In fact, the ABC Conjecture is based upon this idea:

General Question: *In general, how much smaller is the radical of a number than the number itself?*

Are most numbers going to be unaffected (like 30)? Are they going to be significantly smaller, like 112? Are they somewhere in between? Why is this function considered so "radical", anyway? And why do we use "radical" to mean "awesome!"? And what about the phrase "That's radicool!"? Wasn't that a stupid expression? Who came up with that one? And why? Oh, and remember "Don't have a cow, man!"? What ever happened to that phrase?

These are all very important questions, so a conjecture that merely addressed these questions would have been enough for most people. However, Masser and Oesterle are not most people. They realized that they could come up with a way to merge these questions with other ideas in number theory and make an even more ambitious and sweeping conjecture with broad implications across mathematics. Like midgets at a shooting range for really tall people, Masser and Oesterle decided that it was time to aim high....

Chapter 3

Towards A Meaningful ABC

3.1 Fixing the Conjecture So That Masser Can Throw Up On It Again

When Masser and Oesterle stumbled upon these questions, they realized that it was a golden opportunity to not only say something interesting about the radical function but also to say something about equations themselves.

To explain, let's go back to the equation we discussed earlier:

$$a + b = c.$$

Here, I'm going to require that a, b, and c all be positive integers so that we don't have to deal with negatives or zeroes or fractions or imaginary numbers or radicals or whatever else because, seriously, the hell with that crap. The numbers here will be whole, they will be positive, and they will be fantastic.

In fact, I'm going to assume that a, b, and c don't have any common factors (besides 1), because numbers in an equation having common factors is like the mathematical version of inbreeding; it's disgusting, and everything that comes out is dumber because of it. And that's all I'll say about that.

Now that we've gotten those unpleasantries out of the way, we have the following question:

New, Improved ABC Question: *Take the equation from above:*

$$a + b = c,$$

where a, b, and c don't have any common factors. How to a, b, and c compare to rad(abc)?

Now, why does this help, apart from the fact that we've eliminated the unsavory practice of inbreeding in mathematics? Well, it turns out that this is a really, really clever way to take an average; although it's entirely possible that one of the numbers in the equation might be something like 2^{1320} that gets a pretty big haircut from the radical function[1], it's pretty unlikely that all three of the numbers are going to be that way. Basically, it's the number theory version of taking a random poll; 2^{1320} might have a strong opinion on the radical function, but having two other numbers in the sample help counterbalance 2^{1320} and give a more reasoned answer.[2]

Now, you might be wondering, "In that case, why did you only include three numbers? Most polls have 500 numbers in their sample. Why don't you set up an equation with more variables?"

If you asked this to a number theorist, he or she would probably tell you that three turns out to be enough variables to say something interesting; in fact, he would say, having 500 variables would just be overkill because the result probably wouldn't get that much better. But really, we're just lazy. So...three variables it is.

What's even better about this method, though, is it takes the radical and somehow relates it to equations. This means that we can now apply all of the stuff we know about primes and radicals to cases where we're trying to solve equations. As you might be aware, mathematics has many equations, so this will help out quite a bit.

[1] This comment is much funnier if you envision 2^{1320} as 2 with a giant afro.

[2] Now, you can see why we eliminated numbers that have common factors; they would all be affected similarly by the radical function. For instance, if we took a, b, and c to be something like

$$2^{1320} \cdot 3 + 2^{1320} \cdot 4 = 2^{1320} \cdot 7,$$

you can see that all three of the numbers would be decimated by the radical function.

This would be the mathematical equivalent of taking a poll on presidential approval and choosing all of your participants from Barack Obama's immediate family.

3.2 The Almost-Conjecture

So what can we say about the conjecture? Well, we almost have the following:

Thing That's Not Quite True But is Probably Really Close: *Take $a + b = c$ like before. Then the following isn't actually always true but seems to usually be the case:*

$$c < rad(abc).$$

This actually looks like it's true most of the time (i.e. for most a, b, and c that you plug in), which is at least a start. The problem is that "most of the time" doesn't cut it in mathematics; in our field, "almost true" is a synonym for "false"[3], and if we're going to come up with a conjecture that is going to change the face of mathematics, it would probably help if said conjecture is, you know, not false.

3.3 The Almost Conjecture, But With Less "Almost" and More "Conjecture"

So, how do we fix this and make it true *all* of the time?

Well, one way is to raise the right hand side to a power:

$$c < rad(abc)^{102562}$$

No, no, a smaller power than that.

$$c < rad(abc)^2$$

Yeah, that's better. In fact, we can call that something like the ABC conjecture:

Part of the ABC Conjecture: *Let a, b, and c are positive integers that don't do anything creepy like possess common factors. Oh, and $a + b = c$. If all of that stuff is true then*

[3] Examples of a, b, and c for which this is false are actually rather hard to come by. See if you can come up with one! It'll be fun! Whoo-hoo! (If you don't want to bother, or if you're stumped, one possible answer is at the bottom of the next page)

$$c < rad(abc)^2.$$

Now, this is probably correct (which is why we called it a conjecture instead of something like "Bad Guess"), but it's also probably overkill, akin to washing the dishes with a fire hose. Squaring the right hand side is a powerful operation that makes the term on the right much, much bigger (after all, we said that an exponent of 1 would work for almost all a, b, and c), and we'd like to know if we can get something smaller than 2 in the exponent.

Well, can we? For instance, let's say we wanted to lower the exponent from 2 to 1.5. Could we do that?

Um, sort of...

Another Part of the ABC Conjecture: *Let a, b, and c be good like before. IF C IS SUFFICIENTLY LARGE then*

$$c < rad(abc)^{1.5}.$$

Did you happen to notice that I slipped in a few words there? I tried to be subtle, but my caps lock key got stuck. Oh well.

Anyway, the new words say that this isn't true for *every* a, b, and c, but once c passes a certain threshold, it'll always be true.

It's worth noting that we have absolutely no idea where this threshold is. We know that it's pretty large (we've computed some pretty big numbers where the equation doesn't yet work), but as far as how large we're talking.....no clue. However, even knowing that such a threshold exists would be a big deal; one of the difficulties of math is that we're always trying to show that something is true for every possible number (all the way out to infinity), so if we knew that there was a (finite) threshold where we could stop checking things, that would seriously cut down on the work we have to do and would therefore be awesome.

[3]An answer from the previous page: $5 + 27 = 32$. Note that $27 = 3^3$ and $32 = 2^5$, so

$$rad(5 * 27 * 32) = 5 * 3^{\cancel{3}} * 2^{\cancel{5}} = 30,$$

and $30 < 32$.

3.4 Movin' on Down: What The Jefferson's Theme Song Would Be if You Turned The TV Upside Down[4]

So, throughout the section, we've been working on making that exponent smaller and smaller. Now that we've got this adjustment where we say "for sufficiently large c" and everything is magically better, you might be wondering how much farther we can get this exponent to go. Well, the bad news is that we still can't get it all the way down to 1 - no matter how high the threshold, you can always find an a, b, and c that don't work where c is bigger than your threshold. The good news, though, is that we can get really, really close to 1. In fact, we can get about as close to 1 as you want:

The Full ABC Conjecture: *Let a, b, and c be good like before, and let r be a positive number that's as close to 0 as you like (without being 0). If c is sufficiently large then*

$$c < rad(abc)^{1+r}.$$

Of course, what we mean by sufficiently large will depend on which r we've chosen; the threshold we pick for $r = 0.5$ will be way too small for $r = 0.05$, and what works for $r = 0.05$ probably won't work for $r = 0.0001$. In effect, the ABC Conjecture is not one conjecture but tons and tons of mini-conjectures; for each possible r, you have to both prove the conjecture and find the threshold for which it works. That said, we don't have to get them all at once; if we could prove this for *any* choice of r, it would be a huge advance in mathematics and would give us a lot of new information. Plus, Masser would probably throw up at the celebration party.

[4]Viewer discretion is advised.

Chapter 4

Current State Of Affairs: Where We Are and Things That The ABC Conjecture Would Prove

4.1 How Close Are We to Proving the ABC?

Not very. Remember how the statement was that for sufficiently large c,

$$c < rad(abc)^{1+r}?$$

Well, most of the results we've gotten have looked more like this:

$$c < e^{rad(abc)^{1+r}}.$$

That's not very good. Any time you're raising e to a power, you're making things a whole lot bigger.[1]

In fact, this part's kind of depressing, let's go ahead and skip to the things that the ABC Conjecture would prove. That's way more exciting.

[1] I should add a note here that in September of 2012, Shin Mochizuki announced a possible proof of the theorem. The proof is impressive, and it looks promising (and even if it's wrong, it's still extremely interesting), but many, many, many proofs of the ABC have been proposed so far and none have been correct, so I'll hold off on the coronation for now.

4.2 Things That The ABC Conjecture Would Prove

Much like most of the other conjectures in this book, a proof of the ABC Conjecture would have quite a few effects in other places in number theory. Examples include:

1.) **Fermat's Last Theorem**. For many years, Fermat's Last Theorem was one of the most popular unsolved problems in all of mathematics. I think I've already mentioned it in several places in this book, but it bears stating in some detail here because a.) it's important, and b.) it's one of the most obvious motivations for studying the ABC Conjecture.

As the story goes, when mathematicians were studying Fermat's notes and works after he died in 1665, they found a curious comment scribbled in the margin of Fermat's copy of Diophantus' *Arithmetica*:

$x^n + y^n = z^n$ *has no solutions if* $n > 2$

and, underneath that,

I have a truly marvelous proof of this proposition which this margin is too narrow to contain.

This simple statement set off a three century search for a proof of this proposition, as the conjecture that would go on to be called Fermat's Last Theorem stumped many of the greatest minds in the history of number theory. It was finally solved in 1994 by Andrew Wiles, who wrote a 192 page proof of the theorem, then discovered that the 192 pages weren't quite enough to actually prove the theorem, and finally released an additional 12-page paper that completed the proof. Wiles' proof depended on a method known as "the kitchen sink", where he pretty much took everything in modern mathematics that wasn't bolted down and threw it at the problem and eventually got things to work. It's a very brute force-ish proof - effective, but not efficient by any means[2].

[2]Incidentally, one of the great questions in math history is, "Did Fermat actually have a solution to this problem?" Obviously, the method of proof that Andrew Wiles used was not available to Fermat at the time, so the question is really whether Fermat had a simple,

On the other hand, if the ABC were true, Fermat's Last Theorem could be easily proven in less than a page. That's right, I said *less than a page*. It's that powerful.

Other results include....

2.) **Progress on Wieferich's Primes**. Yeah, there's that. And

2.) **Szpiro's Conjecture About Elliptic Curves**. Is a nice one too. And

3.) **A Result about Class Numbers** is something I would bother explaining, except that....

4.) **Seriously, FERMAT'S F*****G LAST THEOREM**. I mean, I don't even know why I should bother with the other results. A proof of the ABC Conjecture turns the most difficult problem of the last 300 years into an undergraduate classroom exercise. I think I should be able to just stop here.

In fact, I will[3].

---

low-tech proof of this problem. I'm firmly in the "No" camp for two reasons: a.) Fermat is known to have stated theorems that he couldn't actually prove (we know this because he occasionally stated "theorems" that turned out to be false), and b.) if there actually was a simple solution, Euler probably would have figured it out.

[3]A full list of implications of the ABC Conjecture is available at

http://www.math.unicaen.fr/~nitaj/abc.html.

Also available at that website is a blinding, puke-green color background and flashing fonts that make the webpage look like it came straight from 1995.

Chapter 5

Appendix: Why ABC gives us Fermat's Last Theorem

Earlier, I made a statement that ABC would be able to prove Fermat's Last Theorem very, very easily. You might remember it - it was a statement laced with expletives and stuff. Anyway, the more mathematically inclined among you might have said, "That's an awfully bold claim! I'd like to see this purported proof." Actually, the less mathematically inclined among you might have said that, too. I don't know. I'm not really in the business of predicting what people will say.

Anyway, in this section, I wanted to sketch out how this proof would go. If you're afraid of math, no worries - the proof is obviously pretty short and doesn't require any advanced math. (Honestly, that's probably a good description of what's most amazing about this proof - it's short and doesn't require advanced math).

All right, let's do this...

5.1 The First Step: State the Facts

To start out, we're going to need two facts, which I will cleverly label Fact 1 and Fact 2:

Fact 1: The radical of x^n is the same as the radical of x, which makes sense since the radical gets rid of exponents. If we wanted to write this in math, we would say $rad(x^n) = rad(x)$.

Fact 2: $rad(x)$ can't be bigger than x. Of course this is true - the radical function strips exponents, so it either makes your number smaller or keeps it the same. In math language, we would write $rad(x) \leq x$.

Now, let's say we had a solution to our Fermat equation

$$x^n + y^n = z^n.$$

(We'll assume that x, y, and z are all positive.) Then we can add Fact 3:

Fact 3: x and y are both less than z. You add two positive numbers, you get a bigger positive number. That one makes sense.

5.2 Bring on the Conjecture!

Next, it's time to bring in our ABC Conjecture. Remember that the ABC Conjecture said something like

$$c < rad(abc)^2.$$

There were all different variants, but we'll go with this one because it's a nice, round exponent and I don't feel like dealing with decimals.

Let's apply the ABC Conjecture to our Fermat equation. We've got

$$z^n < rad(x^n y^n z^n)^2.$$

Now, we have the following observations:

1.) $rad(x^n y^n z^n)^2$ is the same thing as $rad(xyz)^2$ because of Fact 1 (the radical takes out exponents, so we might as well help it out).

2.) $rad(xyz)^2 \leq (xyz)^2$ because of Fact 2.

3.) x and y are both less than z (Fact 3, represent!). So $(x \cdot y \cdot z)^2 \leq (z \cdot z \cdot z)^2$.

4.) $(z \cdot z \cdot z)^2$ is the same thing as z^6.

5.) Running by the pool is prohibited.

Putting all of these together, we have that

$$z^n < z^6.$$

That's pretty restrictive. Since z is positive (and an integer), what this really means is that n has to be less than 6.

In effect, we've managed to reduce Fermat's Last Theorem down to some very easy cases, since the cases where n is less than 6 aren't all that difficult and were solved by the early 1800's.

Impressive, no?